Approximate quantum error correction for correlated noise

Avraham Ben-Aroya[*]   Amnon Ta-Shma[†]

Abstract

Most of the research done on quantum error correction studies an error model in which each qubit is affected by noise, independently of the other qubits. In this paper we study a different noise model – one in which the noise may be correlated with the qubits it acts upon.

We show both positive and negative results. On the one hand, we show controlled-X errors cannot be *perfectly* corrected, yet can be *approximately* corrected with sub-constant approximation error. On the other hand, we show that no non-trivial quantum error correcting code can approximately correct controlled phase error with sub-constant approximation error.

1 Introduction

One of the reasons for studying quantum error-correcting codes (QECCs) is that they serve as building blocks for fault-tolerant computation, and so might serve one day as central components in an actual implementation of a quantum computer. Much work was done trying to determine the threshold error, beyond which independent noise[1] can be dealt with by fault-tolerant mechanisms (see the Ph.D. theses [Rei06, Ali07] and references therein).

A few years ago there was some debate whether the independent noise model is indeed a realistic noise model for quantum computation or not (see, e.g., [ALZ06]). This question should probably be answered by physicists, and the answer to that is most likely dependent on the actual realization chosen. Yet, while the physicists try to build actual machines, and the theorists try to deal with higher independent noise, it also makes sense to try and extend the qualitative types of errors that can be dealt with. The results in this paper are both optimistic and pessimistic. On the one hand, we show there are noise models that can be approximately corrected but not perfectly corrected, but on the other hand, there is simple correlated noise that cannot even be approximately corrected. It might be interesting to reach a better understanding of what can be approximately corrected. Also, it might be interesting to come up with other relaxations of quantum error correction that deal better with correlated noise.

1.1 Stochastic vs. Adversarial noise

The basic problem we deal with is that of encoding a message such that it can be recovered after being transmitted over a noisy channel. Classically, there are two natural error models: Shannon's independent noise model and Hamming's adversarial noise model. For example, a typical noise model that is dealt with in Shannon's theory, is one where each bit of the transmitted message is flipped with independent probability p, whereas a typical noise model in Hamming's theory is one where the adversary looks at the transmitted message and chooses at most t bits to flip. We stress that the classical *adversarial* noise model allows the adversary to decide which noise operator to apply based on the specific codeword it acts upon.

[1]The independent noise model is a model in which each qubit is affected by noise, with some probability, independently of the other qubits.

Remarkably, there are classical error correcting codes that solve the problem in the adversarial noise model, which are almost as powerful as the best error correcting codes that solve the problem in the independent noise model. For instance, roughly speaking, any code in the independent noise model must satisfy $r \leq 1 - H(p)$, where r is the rate of the code, p is the noise rate. In the adversarial noise model, the Gilbert-Varshamov bound shows there are codes with rate $r = 1 - H(\delta)$ and relative distance δ, though one can uniquely correct only up to half the distance.[2]

1.2 The quantum case

Let us now consider quantum error correcting codes (QECCs). The standard definition of such codes limits the noise to a linear combination of operators, each acting on at most t qubits. A standard argument then shows that a noise operator that acts on n qubits, such that it acts independently on each qubit with probability $p = t/n$, is very close to a linear combination of error operators that act on only, roughly, t qubits. Thus, any quantum error correcting code (QECC) that corrects all errors on at most t qubits, also *approximately* corrects *independent* noise with noise rate about t/n. Therefore, the standard definition of QECCs works well with independent noise.

As we said before, the classical *adversarial* noise model allows the adversary to decide which noise operator to apply based on the specific codeword it acts upon. In the quantum model this amounts to, say, applying a single bit-flip operator based on the specific basis element we are given, or, in quantum computing terminology, applying a controlled bit-flip. Controlled bit-flips are limited (in that they apply only a single X operator) highly correlated (in that they depend on all the qubits of the input) operators. Can QECC correct controlled bit-flip errors? Can QECC *approximately* correct such errors?

1.3 Correcting controlled bit flip errors

Before we proceed, let us first see that a QECC that corrects one qubit error in the standard sense may fail for controlled bit flip errors. Assume we have a quantum code of dimension $|C|$ that is spanned by $|C|$ orthogonal codewords $\{\phi_i\}$, and can correct any noise operator from $\mathcal{E}$ that is applied on any vector $\phi \in \{\phi_i\}$. Specifically, for any noise operator $E \in \mathcal{E}$, the quantum decoding algorithm maps a noisy word $\phi_i' = E\phi_i$ to a product state $\phi_i \otimes |\mathsf{synd}(E)\rangle$, where $\mathsf{synd}(E)$ is the error-syndrome associated with E. Notice that $\mathsf{synd}(E)$ depends on E alone and not on ϕ_i. Then, we can correct errors applied on any state in the vector space *spanned* by the basis vectors $\{\phi_i\}$. To see that, notice that if we start with some linear combination $\sum_{i=1}^k \alpha_i \phi_i$ and we apply the error E on it, then the corrupted word is $\sum_{i=1}^k \alpha_i E\phi_i$, and applying the decoding procedure we get the state $(\sum_{i=1}^k \alpha_i \phi_i) \otimes |\mathsf{synd}(E)\rangle$. Tracing out the syndrome register we recover the original state. This property, however, breaks down for controlled bit flip errors, where the error may depend on the specific codeword ϕ_i. In that case the corrupted word is $\sum_{i=1}^k \alpha_i E_i \phi_i$. If we use the same decoding procedure, and the decoded word is $\sum_{i=1}^k \alpha_i \phi_i \otimes |\mathsf{synd}(E_i)\rangle$ and if we trace out the syndrome register we end up with a state different then the original state.

The above argument shows that if we allow controlled bit-flip errors, then the environment may get information about the codeword, and thus corrupt it. This, by itself, is not yet an impossibility proof, as it is possible that one can find a code that is immune to controlled bit-flip errors. Unfortunately, an easy argument shows that there is no non-trivial QECC that perfectly corrects such errors (see Theorem 3.1). Therefore, while there are asymptotically good QECC in the standard error model, there are no non-trivial QECC correcting controlled *single* bit-flip errors.

1.4 Approximate error-correction

Summarizing the discussion above, we saw that no QECC can *perfectly* correct controlled bit-flip errors. We now ask whether this also holds when we relax the perfect decoding requirement and only require

---

[2]If we allow list-decoding, then almost up to $1 - r$ noise rate can be corrected.

approximate decoding. Namely, suppose we only require that for any codeword ϕ and any allowed error E, decoding $E\phi$ results in a state *close* to ϕ. Can we then correct controlled bit-flip errors?

Somewhat surprisingly we show a positive answer to this question. That is, we show a QECC of arbitrarily high dimension, that can correct any controlled bit-flip error with sub-constant approximation-error (see Theorem 4.2 for a formal statement). This, in particular, shows that there are error models that cannot be perfectly decoded, yet can be approximately decoded. For the proof, we find a large dimension vector space containing only low-sensitive functions.

Having that we increase our expectations and ask whether one can approximately correct, say, any controlled single-qubit error. However, here we show a negative result. We show that no non-trivial QECC can correct controlled phase-errors with only sub-constant approximation error (see Theorem 5.1 for a formal statement). Namely, no non-trivial QECC can handle, even approximately, correlated noise, if the control is in the standard basis and the error is in the phase.

2   Preliminaries

2.1   Quantum error-correcting codes

Let $\mathcal{N}$ denote the Hilbert space of dimension 2^n. $\mathcal{M}$ is a $[n, k]$ quantum error correcting code (QECC) if it is a subspace of $\mathcal{N}$ of dimension $K \geq 2^k$. We call n the *length* of code, and K the *dimension* of the code. For two Hilbert spaces $\mathcal{N}, \mathcal{N}'$, $L(\mathcal{N}, \mathcal{N}')$ denotes the set of linear operators from $\mathcal{N}$ to $\mathcal{N}'$.

Definition 2.1. A code $\mathcal{M}$ *corrects* $\mathcal{E} \subset L(\mathcal{N}, \mathcal{N}')$ if for any two operators $X, Y \in \mathcal{E}$ and any two codewords $\phi_1, \phi_2 \in \mathcal{M}$, if $\phi_1^* \phi_2 = 0$ then $(X\phi_1)^*(Y\phi_2) = 0$.

Fact 2.1 ([KSV02, Section 15.5])**.** *A code $\mathcal{M}$ corrects $\mathcal{E}$ if for any $X, Y \in \mathcal{E}$, defining $E = X^*Y$, there exists a constant $c(E) \in \mathbb{C}$, such that for any two codewords $\phi_1, \phi_2 \in \mathcal{M}$,*

$$\phi_1^* E \phi_2 = c(E) \cdot \phi_1^* \phi_2.$$

A QECC $\mathcal{M}$ corrects t errors if it corrects all linear operators that correlate the environment with at most t qubits. There are *asymptotically good* QECCs, i.e., $[n, k]$ QECCs that correct $t = \Omega(n)$ errors with $n = O(k)$ [ALT01].

2.2   Boolean functions

The influence of a variable x_i on a boolean function $f : \{0, 1\}^n \to \{0, 1\}$ is defined to be

$$\Pr_{x \in \{0,1\}^n}[f(x) \neq f(x \oplus e_i)],$$

where $e_i \in \mathbb{R}^n$ is the i'th vector in the standard basis. The influence of a function is the maximum influence of its variables. Ben-Or and Linial [BL85] showed that there exists a balanced function $\text{Tribes} : \{0, 1\}^n \to \{0, 1\}$ with influence as small as $O(\frac{\log n}{n})$, and Kahn, Kalai and Linial [KKL88] showed that this bound is tight for balanced functions. We extend this notion to complex valued functions. For $g : \{0, 1\}^n \to \mathbb{C}$ let

$$I_i(g) = \mathbf{E}_{x \in \{0,1\}^n} |g(x) - g(x \oplus e_i)|^2$$

and $I(g) = \max_{i \in [n]} I_i(g)$.

We identify a function $g : \{0, 1\}^n \to \mathbb{C}$ with the vector $\sum_{x \in \{0,1\}^n} g(x) |x\rangle$. When we write g we refer to it as a vector in $\mathcal{N}$. When we write $g(x)$ we refer to g as a function $g : \{0, 1\}^n \to \mathbb{C}$ and $g(x) \in \mathbb{C}$.

3 No QECC can perfectly correct controlled bit flips

We now concentrate on the error model that allows any *controlled bit flip* error. Formally, for $i \in [n]$ and $S \subseteq \{0,1\}^{n-1}$ let $E_{i,S}$ be the operator that applies X on the i'th qubit conditioned on the other qubits being in S. More precisely, we define the operator $E_{i,S}$ on the basis $\{|x\rangle \mid x \in \{0,1\}^n\}$ and extend it linearly. For $x \in \{0,1\}^n$ define $\widehat{x}_i = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in \{0,1\}^{n-1}$. Also, let $X^i \in L(\mathcal{N}, \mathcal{N})$ denote the operator that flips the i'th qubit, i.e., $X^i = I^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}$. Then

$$E_{i,S}|x\rangle = \begin{cases} X^i|x\rangle & \text{if } \widehat{x}_i \in S \\ |x\rangle & \text{otherwise.} \end{cases}$$

Let

$$\mathcal{E}_{\mathbf{cbit}} \stackrel{\text{def}}{=} \left\{ E_{i,S} \mid i \in [n],\ S \subseteq \{0,1\}^{n-1} \right\}.$$

We also define a tiny subset $\mathcal{E}_{\mathbf{singeltons}}$ of $\mathcal{E}_{\mathbf{cbit}}$ by

$$\mathcal{E}_{\mathbf{singeltons}} \stackrel{\text{def}}{=} \left\{ E_{i,\{j\}} \mid i \in [n],\ j \in \{0,1\}^{n-1} \right\}.$$

We claim that even this set of errors *cannot* be corrected.

Theorem 3.1. *There is no QECC with dimension bigger than one that can correct $\mathcal{E}_{\mathbf{singeltons}}$.*

Proof: Suppose there exists a $[n,k]$ code with $k \geq 1$ that corrects $\mathcal{E}_{\mathbf{singeltons}}$. Let $\phi = \sum_{i \in \{0,1\}^n} \phi(i)|i\rangle$ and $\psi = \sum_{i \in \{0,1\}^n} \psi(i)|i\rangle$ be two orthonormal codewords. We will prove that:

Claim. *For every $i \in [n]$ and every $q \in \{0,1\}^n$ it holds that $\phi(q) = \phi(q \oplus e_i)$.*

In particular, it follows that $\phi = \alpha \cdot \sum_{i \in \{0,1\}^n}|i\rangle$ for some $0 \neq \alpha \in \mathbb{C}$. Similarly, $\psi = \alpha' \cdot \sum_{i \in \{0,1\}^n}|i\rangle$ for some $0 \neq \alpha' \in \mathbb{C}$. Therefore, $\phi^*\psi = 2^n \alpha^* \alpha' \neq 0$. A contradiction.

We now prove the claim. Fix $i \in [n]$ and $q \in \{0,1\}^n$. Denote $E = E_{i,\{q\}}$ and $q' = q \oplus e_i$. It can be verified that

$$
\begin{aligned}
\phi^*E\phi &= \phi^*\phi - |\phi(q) - \phi(q')|^2 = 1 - |\phi(q) - \phi(q')|^2 \\
\psi^*E\psi &= \psi^*\psi - |\psi(q) - \psi(q')|^2 = 1 - |\psi(q) - \psi(q')|^2 \\
\psi^*E\phi &= -(\phi(q) - \phi(q'))^*(\psi(q) - \psi(q'))
\end{aligned}
$$

As $\phi^*\psi = 0$, by the QECC definition, $\psi^*E\phi = 0$ and so $(\phi(q) - \phi(q'))^*(\psi(q) - \psi(q')) = 0$. If $\phi(q) \neq \phi(q')$ we conclude that $\psi(q) = \psi(q')$. But then, $\phi^*E\phi < 1$ while $\psi^*E\psi = 1$, which contradicts Fact 2.1. Therefore, $\phi(q) = \phi(q')$. ∎

The argument above shows that for any $w, w' \in \{0,1\}^n$ and any codeword ϕ, $\phi(w) = \phi(w')$, by employing a sequence of *small* changes, and showing that ϕ is invariant under these small changes. However, if we replace the stringent notion perfect decoding with the more relaxed notion of *approximate decoding*, then at least theoretically it is possible that under this weaker notion, controlled bit flips can be corrected. Somewhat surprisingly, this is indeed the case.

4 An approximate QECC for controlled bit flips

We first define a relaxed notion of error-detection. We say a code *separates* $\mathcal{E}$ if for any two allowed errors $X, Y \in \mathcal{E}$ and any two orthogonal codewords ϕ, ψ, $X\phi$ and $Y\psi$ are far away from each other. Formally,

Definition 4.1. Let $\mathcal{M} \subseteq \mathcal{N}$ be an $[n,k]$ QECC and $\mathcal{E} \subset L(\mathcal{N}, \mathcal{N}')$. We say $\mathcal{M}$ separates $\mathcal{E}$ with at most α error, if for any two operators $X, Y \in \mathcal{E}$ and any two unit vectors $\phi_1, \phi_2 \in \mathcal{M}$, if $\phi_1^*\phi_2 = 0$ then $|\phi_1^*X^*Y\phi_2| \leq \alpha$.

We say a code $\mathcal{M}$ *approximately* corrects $\mathcal{E}$ if there exists a POVM on $\mathcal{N}'$ such that for any operator $X \in \mathcal{E}$, and any codeword $\phi \in \mathcal{M}$, when we apply the POVM on $X\phi$, the resulting mixed state is close to the pure state ϕ. A very special case of the above is when the decoding procedure is the *identity* function. In this case we say $\mathcal{M}$ is $(\mathcal{E}, \varepsilon)$ *immune*. Formally,

Definition 4.2. Let $\mathcal{M} \subseteq \mathcal{N}$ be an $[n, k]$ QECC and $\mathcal{E} \subset L(\mathcal{N}, \mathcal{N}')$. We say $\mathcal{M}$ is $(\mathcal{E}, \varepsilon)$ immune if for every $X \in \mathcal{E}$ and every $\phi \in \mathcal{M}$, $|\phi^* X \phi| \geq (1 - \varepsilon)|\phi^* \phi|$. We call ε the *approximation error*.

We saw before that there is no non-trivial QECC that perfectly corrects $\mathcal{E}_{\mathbf{cbit}}$. In contrast, we will now construct a large QECC that is immune against $\mathcal{E}_{\mathbf{cbit}}$, with sub-constant approximation error.

4.1 The construction

The calculations done in Section 3 can be generalized to show that if we want ϕ to be ε-immune for bit flip errors, then $\phi(x)$ must have low influence. However, we also want the QECC to have a large dimension, and so we want many orthogonal such vectors. The idea is to work with a function f of low influence, and combine it on many independent blocks.

Pick an integer B such that $2B$ divides n, and define $n' = \frac{n}{2B}$. Fix a balanced function $f : \{0, 1\}^{n'} \to \{\pm \frac{1}{2}\}$ with low influence, i.e., $I(f) \leq s = s(n')$. We remind the reader that this means that for all j in $[n']$, $I_j(f) = \mathbf{E}_{x \in \{0,1\}^{n'}} |f(x) - f(x \oplus e_j)|^2 \leq s$ (see Section 2). Notice that this implies that for all $j \in [n']$,

$$\Pr_{w \in \{0,1\}^{n'}} [f(w) \neq f(w \oplus e_j)] \leq s. \tag{1}$$

We use the low-influence function f as a building block.

Now partition $[n]$ into $2B$ blocks of equal length n'. For $x \in \{0, 1\}^n$, $i \in \{1, \ldots, B\}$ and $b \in \{0, 1\}$, let $x_{i,b} \in \{0, 1\}^{n'}$ denote the value of x restricted to the $(2i - 1 + b)$'th block, i.e., the string x is the concatenation of the blocks $x_{1,0}, x_{1,1}, x_{2,0}, x_{2,1}, x_{3,0}, \ldots, x_{B,0}, x_{B,1}$. For $z = (z_1, \ldots, z_B) \in \{0, 1\}^B$ we define a function $f_z : \{0, 1\}^n \to \mathbb{C}$ that apply f on the blocks corresponding to z. That is,

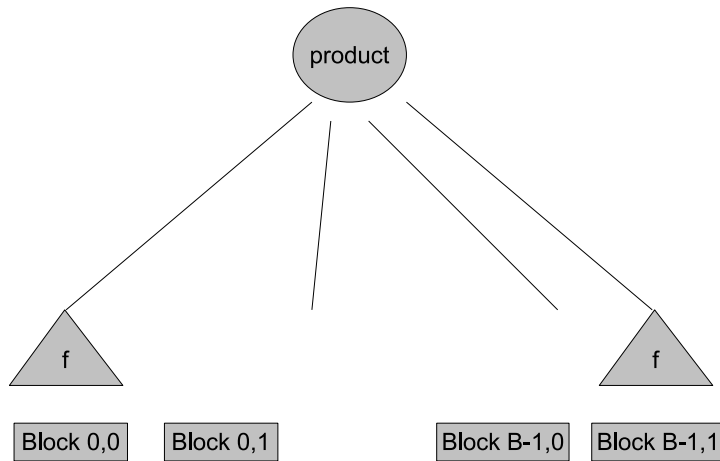$$f_z(x) = f(x_{1,z_1}) \cdot \ldots \cdot f(x_{B,z_B}),$$

as shown in Figure 1.

Figure 1: *The input is B pairs of blocks, each block is of length n'. The values $z_1, \ldots, z_B \in \{0, 1\}^B$ determine on which block in each pair f is applied. In the example, $z_1 = 0$ while $z_B = 1$. The output is the product of the B values.*

As usual we look at f_z as a vector in $\mathcal{N}$. We let $W = \mathrm{Span}\left\{f_z : z \in \{0, 1\}^B\right\}$. We claim:

Theorem 4.1. W is an $[n, B]$ QECC that is $(\mathcal{E}_{\mathbf{cbit}}, 2s(n'))$ immune.

In particular, taking $f(w) = \frac{1}{2}$ when $\mathsf{Tribes}(w) = 1$ and $f(w) = -\frac{1}{2}$ when $\mathsf{Tribes}(w) = 0$, we get:

Theorem 4.2. *For every $0 < B = B(n) < n$ there exists an $[n, B]$ QECC that is $(\mathcal{E}_{\mathbf{cbit}}, \varepsilon = O(\frac{B \log n}{n}))$ immune.*

In particular, there exists QECCs of length n and dimension $2^{\sqrt{n}}$ that approximately corrects all controlled-X errors with an $O(\frac{\log(n)}{\sqrt{n}})$ approximation error.

4.2 The analysis

We first show that $\dim W = B$. This immediately follows from:

Claim. $\{f_z\}_{z \in \{0,1\}^B}$ *is an orthogonal set.*

Proof: We will show that for $z \neq z'$, $f_z^* f_{z'} = 0$. For that, it is enough to show that $\{(f_z(x), f_{z'}(x))\}_{x \in \{0,1\}^n}$ is uniform over $\{\pm 2^{-B}\} \times \{\pm 2^{-B}\}$.

To see that, first notice that $f(x_{1,i_1})$ is balanced over $\{\pm \frac{1}{2}\}$. Hence, $\{f_z(x)\}_{x \in \{0,1\}^n}$ is uniform over $\{\pm 2^{-B}\}$. Also, as $z \neq z'$ there exists some k such that $z_k \neq z'_k$. Notice that $f(x_{k,z_k})$ depends on bits that do not influence $f_{z'}(x)$, hence it is independent of $f_{z'}(x)$. It is also uniform on $\{\pm \frac{1}{2}\}$. Hence the pair $(f_z(x), f_{z'}(x))$ is uniform over $(\pm 2^{-B}, \pm 2^{-B})$ as desired. ∎

We now analyze the approximation error. We will use the following lemmas:

Lemma 4.3. *For every $\phi \in \mathcal{N}$ and every $i \in [n]$, $S \subseteq \{0,1\}^{n-1}$,*

$$|\phi^* E_{i,S} \phi - \phi^* \phi| \leq 2^{n-1} I_i(\phi).$$

Lemma 4.4. *For every $\phi \in W$,*
$$2^{n-1} I(\phi) \leq 2s \cdot |\phi^* \phi|.$$

These lemmas together imply Theorem 4.1. Notice that in Lemma 4.4 we had to prove the claim for every $\phi \in W$ and not just for some basis of W (see the discussion in the introduction).

Proof of Lemma 4.3: For every $g, h : \{0,1\}^n \to \mathbb{C}$ and every $i \in [n]$, $S \subseteq \{0,1\}^{n-1}$,

$$
\begin{aligned}
h^* E_{i,S} g &= \sum_{x : \widehat{x}_i \notin S} h(x)^* g(x) + \sum_{x : \widehat{x}_i \in S} h(x)^* g(x \oplus e_i) \\
&= \sum_{x \in \{0,1\}^n} h(x)^* g(x) + \sum_{x : \widehat{x}_i \in S} [h(x)^* g(x \oplus e_i) - h(x)^* g(x)].
\end{aligned}
$$

Now, fix i. For $y \in \{0,1\}^{n-1}$ and $b \in \{0,1\}$ let (y, b) denote the string $x \in \{0,1\}^n$ such that $\widehat{x}_i = y$ and $x_i = b$. Then,

$$
\begin{aligned}
|h^* E_{i,S} g - h^* g| &= \left| \sum_{y \in S} (h(y,0)^* - h(y,1)^*)(g(y,0) - g(y,1)) \right| \\
&\leq \sqrt{\sum_{y \in S} |h(y,0)^* - h(y,1)^*|^2} \sqrt{\sum_{y \in S} |g(y,0) - g(y,1)|^2} \\
&\leq \sqrt{\sum_{y \in \{0,1\}^{n-1}} |h(y,0)^* - h(y,1)^*|^2} \sqrt{\sum_{y \in \{0,1\}^{n-1}} |g(y,0) - g(y,1)|^2} \\
&= \sqrt{2^{n-1} I_i(h)} \sqrt{2^{n-1} I_i(g)}
\end{aligned}
$$

∎

6

We now turn to Lemma 4.4. One can check that all elements in $\{f_z\}$ have low influence. However, this by itself does not imply that all elements in W are so. So we verify this directly.

Proof of Lemma 4.4: We want to show that any $\phi \in W$ has low influence. Fix $i \in [n]$ and suppose that i corresponds the j'th variable in the (k, b)'th block. For $x \in \{0,1\}^n$ let $x = (x^{(1)}, x^{(2)})$ where $x^{(2)} = x_{k,b}$ and $x^{(1)} \in \{0,1\}^{n-n'}$ is the rest of x. Let $\widehat{f}_z : \{0,1\}^n \to \mathbb{C}$ be

$$\widehat{f}_z(x) = f(x_{1,z_1}) \cdot \ldots \cdot f(x_{k-1,z_{k-1}}) \cdot f(x_{k+1,z_{k+1}}) \cdot \ldots \cdot f(x_{B,z_B}).$$

Notice that $\widehat{f}_z(x^{(1)}, x^{(2)})$ depends only on $x^{(1)}$. For that reason we also write it as $\widehat{f}_z(x^{(1)})$.

We are given $\phi \in W$ and express it as $\phi = \sum_z \alpha_z f_z$. We want to bound

$$\begin{aligned} I_i(\phi) &= \mathbf{E}_{x \in \{0,1\}^n} |\phi(x) - \phi(x \oplus e_i)|^2 \\ &= \mathbf{E}_{x \in \{0,1\}^n} \left| \sum_z \alpha_z (f_z(x) - f_z(x \oplus e_i)) \right|^2. \end{aligned}$$

The functions f_z for which $f_z(x) = f_z(x \oplus e_i)$ do not contribute to the sum. We can therefore define $\zeta = \sum_{z:z_k=b} \alpha_z f_z$ and it follows that $I_i(\phi) = I_i(\zeta)$. Then,

$$\begin{aligned} 2^{n-1} I_i(\zeta) &= \frac{1}{2} \sum_{x \in \{0,1\}^n} \left| \sum_{z:z_k=b} \alpha_z (f_z(x) - f_z(x \oplus e_i)) \right|^2 \\ &= \frac{1}{2} \sum_{(x^{(1)},x^{(2)}) \in \{0,1\}^n} \left| \sum_{z:z_k=b} \alpha_z \widehat{f}_z(x^{(1)})(f(x^{(2)}) - f(x^{(2)} \oplus e_j)) \right|^2 \\ &= \frac{1}{2} \sum_{(x^{(1)},x^{(2)}) \in \{0,1\}^n} |f(x^{(2)}) - f(x^{(2)} \oplus e_j)|^2 \cdot \left| \sum_{z:z_k=b} \alpha_z \widehat{f}_z(x^{(1)}) \right|^2. \end{aligned}$$

Next, observe that the only terms that contribute non-zero values are those $x = (x^{(1)}, x^{(2)})$ where $f(x^{(2)}) \neq f(x^{(2)} \oplus e_j)$. There are at most $s2^{n'}$ such strings $x^{(2)}$ (see Equation (1)). Also, each such term contributes $|\sum_{z:z_k=b} \alpha_z \widehat{f}_z(x^{(1)})|^2$. However,

$$\begin{aligned} |\zeta(x^{(1)}, x^{(2)})|^2 &= \left| \sum_{z:z_k=b} \alpha_z f_z(x^{(1)}, x^{(2)}) \right|^2 = \left| \sum_{z:z_k=b} \alpha_z \widehat{f}_z(x^{(1)}) f(x^{(2)}) \right|^2 \\ &= |f(x^{(2)})|^2 \cdot \left| \sum_{z:z_k=b} \alpha_z \widehat{f}_z(x^{(1)}) \right|^2 = \frac{1}{4} \left| \sum_{z:z_k=b} \alpha_z \widehat{f}_z(x^{(1)}) \right|^2. \end{aligned}$$

Thus, the term $|\zeta(x^{(1)}, x^{(2)})|^2$ depends only on $x^{(1)}$ and not on $x^{(2)}$, and we denote it by $|\zeta(x^{(1)})|^2$. Denote $\widehat{\zeta} = \sum_{z:z_k=b} \alpha_z \widehat{f}_z$. Notice that $\sum_{x^{(1)}} |\zeta(x^{(1)})|^2 = |\widehat{\zeta}^* \widehat{\zeta}|$. Also, because $\zeta(x^{(1)}, x^{(2)})$ does not depend on $x^{(2)}$, $|\zeta^* \zeta| = 2^{n'} |\widehat{\zeta}^* \widehat{\zeta}|$. Altogether,

$$2^{n-1} I_i(\zeta) = \frac{1}{2} \sum_{x_1} s2^{n'} 4 |\zeta(x_1)|^2 = 2s \cdot 2^{n'} |\widehat{\zeta}^* \widehat{\zeta}| = 2s |\zeta^* \zeta|.$$

Finally, $\zeta = \sum_{z:z_k=b} \alpha_z f_z$ is a linear combination of orthogonal functions $\{f_z\}$ and $|f_z^* f_z| = 2^{n-2B}$. Thus,

$$|\zeta^* \zeta| = \sum_{z:z_k=b} |\alpha_z|^2 2^{n-2B} \leq 2^{n-2B} \sum_z |\alpha_z|^2 = |\phi^* \phi|,$$

which completes the proof. ∎

5 No approximate QECC can correct controlled phase errors

So far we have seen that one can approximately correct controlled-X errors with a sub-constant approximation error. We now show there is no way to correct controlled-phase errors. The reason is that if ϕ and ψ are two orthogonal codewords, then by applying controlled phase errors we can match the phase of ϕ and ψ on any basis vector $|x\rangle$, and this implies that $|\phi^* X \psi|$ is about $\sum_x |\phi(x)| \cdot |\psi(x)|$ which leads to a simple contradiction.

We now formally define our error model. As before, the error operators are linear and hence it is sufficient to define them on the standard basis $\{|x\rangle\}_{x \in \{0,1\}^n}$. We define the error operators $E_{S,\theta}$, for $S \subseteq \{0,1\}^n$ and $\theta \in [2\pi]$ by:

$$E_{S,\theta} |x\rangle = \begin{cases} e^{\theta i} |x\rangle & \text{if } x \in S \\ |x\rangle & \text{otherwise.} \end{cases}$$

In fact, we do not even need to allow any controlled phase error, and we can be satisfied with $\theta \in \{0, \frac{\pi}{4}, \frac{\pi}{2}\}$. Set,

$$\mathcal{E}_{\mathbf{cphase}} = \left\{ E_{S,\theta} \mid S \subseteq \{0,1\}^n, \theta \in \left\{ 0, \frac{\pi}{4}, \frac{\pi}{2} \right\} \right\}.$$

We now prove that such errors cannot be approximately corrected, even for some fixed constant error. In fact, we prove that such errors cannot even be *separated*.

Theorem 5.1. *There is no two-dimensional QECC that separates $\mathcal{E}_{\mathbf{cphase}}$ with at most $\alpha = \frac{1}{10}$ error.*

Proof: Assume $\mathcal{M}$ be a 2-dimensional QECC that separates $\mathcal{E}_{\mathbf{cphase}}$ with at most α error.

Lemma 5.2. *Let $\mathcal{M} \subseteq \mathcal{N}$ be a vector space of dimension greater than one. Then there are two orthonormal vectors $\phi, \psi \in \mathcal{M}$ such that $\sum_x |\phi(x)| \cdot |\psi(x)| \geq \frac{1}{2}$.*

We postpone the proof for later. Fix ϕ and ψ as in the lemma. Notice that by ranging over all $X, Y \in \mathcal{E}_{\mathbf{cphase}}$, we can implement any operator E that partitions $\{0,1\}^n$ to four sets, and based on the set does a phase shift of angle $0, \frac{\pi}{4}, \frac{\pi}{2}$ or $\frac{3\pi}{4}$. More precisely: for a partition $\overline{S} = (S_1, \ldots, S_\ell)$ of $\{0,1\}^n$ and for a tuple of angles $\Theta = (\theta_1, \ldots, \theta_\ell) \subseteq [2\pi]^\ell$ define $E_{\overline{S}, \Theta}$ by $E_{\overline{S}, \Theta} |x\rangle = e^{\theta_j i} |x\rangle$, where j is such that $x \in S_j$. Let $\Theta_k = \left(0, \frac{1}{2^k}\pi, \ldots, \frac{(2^k-1)}{2^k}\pi\right)$ and

$$\mathcal{E}_{\mathbf{cphase}_k} = \left\{ E_{\overline{S}, \Theta_k} \mid \overline{S} = (S_1, \ldots, S_{2^k}) \text{ is a partition of } \{0,1\}^n \right\}.$$

Then, by ranging over all $X, Y \in \mathcal{E}_{\mathbf{cphase}}$ we range over all $E \in \mathcal{E}_{\mathbf{cphase}_2}$. We claim:

Lemma 5.3. *Let $k \geq 1$ and $\varepsilon = 2^{-k}\pi$. For every $\phi, \psi \in \mathcal{N}$ there exists $E \in \mathcal{E}_{\mathbf{cphase}_k}$ such that*

$$|\phi^* E \psi| \geq (1 - \varepsilon) \sum_x |\phi(x)| \cdot |\psi(x)|.$$

Thus, in particular for the ϕ and ψ we fixed before (and setting $k = 2, \varepsilon = \frac{\pi}{4}$):

$$\alpha \geq |\phi^* X \psi| \geq \frac{1 - \varepsilon}{2} > \frac{1}{10}.$$

∎

We are left to prove the two lemmas:

Proof of Lemma 5.2: Let $\phi, \psi \in \mathcal{M}$ be arbitrary orthonormal vectors. Let $\phi' = \frac{1}{\sqrt{2}}(\phi + \psi)$ and $\psi' = \frac{1}{\sqrt{2}}(\phi - \psi)$. Then

$$\sum_x |\phi'(x)| \cdot |\psi'(x)| \quad = \quad \frac{1}{2}\sum_x |\phi(x) + \psi(x)| \cdot |\phi(x) - \psi(x)|.$$

Fix some $x \in \{0,1\}^n$. Denote $a = \phi(x), b = \psi(x)$, $a, b \in \mathbb{C}$ and assume $|a| \geq |b|$. Then,

$$
\begin{aligned}
|(a+b)(a-b)| \quad &= \quad |a^2 - b^2| \geq |a|^2 - |b|^2 = (|a| - |b|)(|a| + |b|) \\
&\geq \quad (|a| - |b|)^2 = |a|^2 + |b|^2 - 2|a| \cdot |b|.
\end{aligned}
$$

Therefore,

$$\sum_x |\phi'(x)| \cdot |\psi'(x)| \quad \geq \quad \frac{1}{2}\sum_x \left(|\phi(x)|^2 + |\psi(x)|^2\right) - \sum_x |\phi(x)| \cdot |\psi(x)| = 1 - \sum_x |\phi(x)| \cdot |\psi(x)|.$$

Thus, either $\sum_x |\phi(x)| \cdot |\psi(x)|$ or $\sum_x |\phi'(x)| \cdot |\psi'(x)|$ is at least half. ∎

Proof of Lemma 5.3: Express $\phi(x) = r_x \cdot e^{\theta_x i}$ with $r_x = |\phi(x)| \in R^+$ and $\theta_x \in [2\pi]$. Similarly, $\psi(x) = r'_x \cdot e^{\theta'_x i}$. The partition $\overline{S} = (S_1, \ldots, S_{2^k})$ is defined as follows. For every x we look at $\min_j \{|\theta'_x + \theta_j - \theta_x|\}$. Any x is chosen to be in $S_{j'}$ according to the j' that minimizes the above expression for that x. Note that the above expression is always bounded by $2^{-k}\pi$.

Denote $E = E_{\overline{S}, \Theta_k}$. Then,

$$|\phi^* E \psi| = \left| \sum_x r_x r'_x e^{\zeta_x i} \right|,$$

where $|\zeta_x| \leq 2^{-k}\pi$. Let $u_x = 1 - e^{\zeta_x i}$ and notice that

$$|u_x|^2 = 2(1 - \cos(\zeta_x)) \leq \zeta_x^2 \leq 2^{-2k}\pi^2$$

and $|u_x| \leq 2^{-k}\pi = \varepsilon$. Thus,

$$
\begin{aligned}
|\phi^* E \psi| \quad &= \quad \left| \sum_x r_x r'_x (1 - u_x) \right| \geq \sum_x r_x r'_x - \left| \sum_x r_x r'_x u_x \right| \\
&\geq \quad (1 - \max_x |u_x|) \sum_x r_x r'_x \geq (1 - \varepsilon) \sum_x r_x r'_x,
\end{aligned}
$$

as desired. ∎

References

[Ali07]   P. Aliferis. *Level Reduction and the Quantum Threshold Theorem*. PhD thesis, California Institute of Technology, 2007. Arxiv preprint: quant-ph/0703230.

[ALT01]   A. Ashikhmin, S. Litsyn, and M.A. Tsfasman. Asymptotically good quantum codes. *Physical Review A*, 63(3):32311, 2001.

[ALZ06]   R. Alicki, D.A. Lidar, and P. Zanardi. Internal consistency of fault-tolerant quantum error correction in light of rigorous derivations of the quantum Markovian limit. *Physical Review A*, 73(5):52311, 2006.

[BL85]   M. Ben-Or and N. Linial. Collective coin flipping, robust voting schemes and minima of Banzhaf values. In *Proceedings of 26th IEEE FOCS*, pages 408–416, 1985.

[KKL88] J. Kahn, G. Kalai, and N. Linial. The influence of variables on Boolean functions. In *Proceedings of 29th IEEE FOCS*, pages 68–80, 1988.

[KSV02] A.Y. Kitaev, A. Shen, and M.N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[Rei06] B. Reichardt. *Error-detection-based quantum fault tolerance against discrete Pauli noise*. PhD thesis, UC Berkeley, 2006. Arxiv preprint quant-ph/0612004.